

REMARKS

In response to the Advisory Action and earlier Office Action, this Response is being filed along with a Request for Continued Examination (RCE).

Claims 4 to 9 are pending in the present application.

Applicants respectfully request reconsideration of the present application in view of this response.

In a previous Office Action, claims 4 to 9 were rejected under 35 U.S.C. §102(b) as anticipated by U.S. Patent No. 5,825,300 to Bathrick et al. ("Bathrick reference").

Applicants respectfully submit that the Bathrick reference does not identically describe or suggest the present application as claimed. The Bathrick reference is believed to teach a fundamentally different system than that claimed in the present application. In its specification, the Bathrick reference purportedly describes a shared secret system. The present application does not employ a shared secret system, thus providing a more robust system since if a secret is broken, only one side is affected. Further, the Bathrick reference purportedly describes using a public key which is protected by an address or such authentication means. The present application does not need to provide protection for a public key, thus no address is needed for authentication as in the Bathrick reference. In the present application, the public key is generated and no one knows the public key, and no one needs any authentication address, because the public key issued by the trust center shows the information that it is coming from the correct user. Essentially, the public key protects itself – in direct contrast to the system in the Bathrick reference. There are several additional stark differences between the old system described in the Bathrick reference and the new invention claimed in the present application (including, for example, in Bathrick reference, a user is apparently provided with keying materials and a password; and, in the present application a user is provided with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair; Bathrick does not user a crypto key, etc.). See, for example, columns 2 and 3 of the Bathrick reference. Applicants' comments in earlier responses concerning the present application are respectfully incorporated herein by reference.

In contrast, claim 4 of the present invention concerns a method for generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location correspondence to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center. The Bathrick reference does not *identically* disclose (as it must for anticipation) or suggest at least the features of causing *the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair; unequivocally assigning the at least*

one encryption key pair to the user; causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair; after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair; and encrypting the new certificate using the public part of the at least one encryption key pair.

Accordingly, Applicants respectfully submit that the Bathrick reference does not anticipate claim 4. Claim 7 recites features analogous to those of claim 4 and is therefore allowable for essentially the same reasons as claim 4. Claims 5, 6, 8, and 9, depend from one of claims 4 and 7, and are allowable for the same reasons.

In summary, it is respectfully submitted that all of claims 4 to 9 of the above-identified present application are allowable for the foregoing reasons.

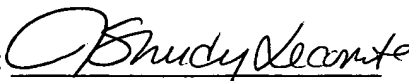
CONCLUSION

In view of all of the above, it is believed that all claims 4 to 9 are allowable. It is therefore respectfully requested that any outstanding rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

If it would further allowance of the present application, the Examiner is invited to contact the undersigned.

Respectfully submitted,

Dated: Jan 29, 2007

By: 
Linda Shudy Lecomte
(Reg. No. 47,084)

CUSTOMER NO. 26646

KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200